

Security bound of cheat sensitive quantum bit commitment

Guang Ping He*

School of Physics and Engineering, Sun Yat-sen University, Guangzhou 510275, China

Cheat sensitive quantum bit commitment (CSQBC) loosens the security requirement of quantum bit commitment (QBC), so that the existing impossibility proofs of unconditionally secure QBC can be evaded. But here we analyze the common features in all existing CSQBC protocols, and show that in any CSQBC having these features, the receiver can always learn a non-trivial amount of information on the sender's committed bit before it is unveiled, while his cheating can pass the security check with a probability not less than 50%. The sender's cheating is also studied. The optimal CSQBC protocols that can minimize the sum of the cheating probabilities of both parties are found to be trivial, as they are practically useless. We also discuss the possibility of building a fair protocol in which both parties can cheat with equal probabilities.

PACS numbers: 03.67.Dd, 89.70.-a, 03.67.Mn, 03.65.Ud

Quantum bit commitment (QBC) is a two-party cryptography including the following phases. In the commit phase, Alice (the sender of the commitment) decides the value of the bit b ($b = 0$ or 1) that she wants to commit, and sends Bob (the receiver of the commitment) a piece of evidence, e.g., some quantum states. Later, in the unveil phase, Alice announces the value of b , and Bob checks it with the evidence. The interval between the commit and unveil phases is sometimes called the holding phase. A QBC protocol is called unconditionally secure if any cheating can be detected with a probability arbitrarily close to 1. Here Alice's cheating means that she wants to change the value of b after the commit phase, while Bob's cheating means that he tries to learn b before the unveil phase.

QBC is an essential primitive for building quantum multi-party secure computations and other "post-cold-war era" multi-party cryptographic protocols [1, 2]. Unfortunately, it is widely believed that unconditionally secure QBC is impossible [3, 4]. This result, known as the Mayers-Lo-Chau (MLC) no-go theorem, was considered as putting a serious drawback on quantum cryptography.

To evade the problem, the concept "cheat sensitive quantum bit commitment (CSQBC)" was proposed [5–10], where the probability for detecting the cheating does not need to be arbitrarily close to 1. Instead, it merely requires the probability to be nonzero. With this loosen security requirement, many insecure QBC protocols can be regarded as secure CSQBC. Therefore, at the first glance it seems that CSQBC will be very easy to achieve.

But intriguingly, here we will show that there still exists boundary for the security of a typical class of CSQBC. Especially, Bob can always feel free to measure the quantum states to learn b , while he stands at least 50% chances to escape Alice's detection.

Result

Common features of CSQBC

By checking the existing CSQBC protocols [5–10], we find that they all share the following common features (note that the names Alice and Bob are used reversely in [7, 9, 10]):

(1) During the holding phase, the receiver Bob owns a quantum system Ψ encoding Alice's committed bit b . (Ψ can either be prepared by the sender Alice, or be prepared by Bob and sent to Alice, who returns it to Bob after performing some certain operations according to her choice of b . It also does not matter whether Alice prepared and kept another quantum system entangling with Ψ .)

(2) Bob knows the definitions of ρ_0^B and ρ_1^B directly before the end of the commit phase. (That is, these definitions are either clearly stated by the protocol, or announced to Bob by Alice classically. Bob does not need to perform operations on any quantum system to gain knowledge of these definitions.) Here ρ_0^B and ρ_1^B are the density matrices of Bob's Ψ corresponding to $b = 0$ and $b = 1$, respectively.

(3) To detect Bob's cheating, at the unveil phase Alice can check whether the state of Ψ is intact. (It does not matter whether the entire Ψ or only a small part can be checked.)

(4) To detect Alice's cheating, at the unveil phase Bob can learn a nontrivial amount of information on the value of b from Ψ , even without any help from Alice.

The last feature indicates that there exists at least one operation known to Bob, which can output a bit b' when being applied on Ψ , and $b' = b$ should occur with a probability larger than $1/2$. As a result, there must be $\rho_0^B \neq \rho_1^B$. This is a main difference from the original QBC, where there is generally $\rho_0^B \simeq \rho_1^B$ so that it can be unconditionally secure against dishonest-Bob.

The original purpose of CSQBC having these features is as follows. Alice's cheating strategy suggested in the MLC no-go theorem is based on the Hughston-Jozsa-

*Electronic address: hegp@mail.sysu.edu.cn

Wootters (HJW) theorem [11], which applies to the case $\rho_0^B \simeq \rho_1^B$. Therefore with feature (4), i.e., $\rho_0^B \neq \rho_1^B$, Alice's cheating becomes detectable so that the MLC no-go theorem can be evaded. On the other hand, if Bob takes advantages of $\rho_0^B \neq \rho_1^B$ and performs measurements to discriminate the committed bit b , the quantum state will be disturbed. In this case, with feature (3) Bob's cheating will be detected with a certain probability when Alice asks him to return the quantum state and checks whether it remains undisturbed, so that the goal of CSQBC can be met.

But with a rigorous quantitative analysis on the probability of detecting Bob's cheating, we will find that it is always not sufficiently large when Bob applies some specific measurements. Therefore any CSQBC protocol having the above four features will be bounded by the security limit below.

Notations and Bob's cheating strategy

According to Eq. (9.22) of [12], the trace distance $D(\rho_0^B, \rho_1^B) \equiv \text{tr} |\rho_0^B - \rho_1^B| / 2$ (where $|A| \equiv \sqrt{A^\dagger A}$) between ρ_0^B and ρ_1^B satisfies

$$D(\rho_0^B, \rho_1^B) = \max_P \text{tr}(P(\rho_0^B - \rho_1^B)), \quad (1)$$

where the maximization is taken over all positive operators $P \leq I$, with I being the identity operator. The above feature (2) of CSQBC guarantees that Bob knows how ρ_0^B and ρ_1^B are defined. Thus he can find the positive projectors $P = P_m$ that maximizes $\text{tr}(P(\rho_0^B - \rho_1^B))$. If ρ_0^B stands a higher probability to be projected successfully than ρ_1^B when applying P_m , then we take $P_0 \equiv P_m$ and $P_1 \equiv I - P_m$. Otherwise we take $P_0 \equiv I - P_m$ and $P_1 \equiv P_m$. Feature (1) ensures that Bob owns the system Ψ encoding Alice's committed bit b during the holding phase. Therefore, by applying the positive operator-valued measure (POVM) $\{P_0^\dagger P_0, P_1^\dagger P_1\}$ on Ψ , Bob can discriminate between ρ_0^B and ρ_1^B and learn Alice's committed b with the maximal probability allowed by $D(\rho_0^B, \rho_1^B)$.

To analyze rigorously the probability for Bob to escape Alice's detection with this POVM, let H be the global Hilbert space constructed by all possible states of Ψ (either $b = 0$ or 1). Since P_0, P_1 are positive projectors, there exists an orthonormal basis $\{|e_i\rangle\}$ of H (the following proof remains valid regardless whether $\{|e_i\rangle\}$ is known to Alice or Bob), in which P_0, P_1 can be expressed as

$$\begin{aligned} P_0 &= \sum_i |e_i^{(0)}\rangle \langle e_i^{(0)}|, \\ P_1 &= \sum_i |e_i^{(1)}\rangle \langle e_i^{(1)}|, \end{aligned} \quad (2)$$

where $\{|e_i^{(0)}\rangle\} \cup \{|e_i^{(1)}\rangle\} = \{|e_i\rangle\}$.

Meanwhile, before Bob applying any measurement, the general form of the initial state of Ψ can always be written as

$$\begin{aligned} |\Phi \otimes \Psi\rangle_{ini} &= \sqrt{\alpha} \sum_i \lambda_i^{(0)} |f_i^{(0)}\rangle \otimes |e_i^{(0)}\rangle \\ &+ \sqrt{\beta} \sum_i \lambda_i^{(1)} |f_i^{(1)}\rangle \otimes |e_i^{(1)}\rangle, \end{aligned} \quad (3)$$

where $0 \leq \alpha \leq 1$, $\beta = 1 - \alpha$, and $\sum_i |\lambda_i^{(0)}|^2 = \sum_i |\lambda_i^{(1)}|^2 = 1$ (sum over all possible i within each corresponding subspace). The values of α , β , $\lambda_i^{(0)}$'s and $\lambda_i^{(1)}$'s are chosen by Alice according to the value of her committed bit b . Here Φ is a quantum system that Alice may introduce and keep to herself, which entangles with Bob's Ψ . All $|f_i^{(0)}\rangle$'s and $|f_i^{(1)}\rangle$'s are the vectors describing the state of Φ , which are not required to be orthogonal to each other. In the case where Alice does not introduce such a system, we can simply set all $|f_i^{(0)}\rangle$'s and $|f_i^{(1)}\rangle$'s to be equal, so that Eq. (3) still applies.

The security bound on Bob's cheating

As elaborated in the 1st subsection of Methods section, when dishonest-Bob applies the above POVM $\{P_0^\dagger P_0, P_1^\dagger P_1\}$ on Ψ , we find that the probability for Bob's cheating to pass Alice's detection successfully is

$$P_B = \frac{1}{2} + \frac{1}{2}(2\alpha - 1)^2, \quad (4)$$

and the amount of mutual information he obtained is

$$I_m = 1 - h(\alpha). \quad (5)$$

Here $h(\alpha) \equiv -\alpha \log_2 \alpha - (1 - \alpha) \log_2 (1 - \alpha)$ is the binary entropy function.

With Eqs. (4) and (5), we plot P_B and I_m as a function of α in FIG. 1. Since $0 \leq \alpha \leq 1$, FIG. 1 and Eq. (4) both gives

$$P_B \geq 50\%. \quad (6)$$

The minimum $P_B = 50\%$ can be reached when Alice chooses $\alpha = 0.5$. Thus we come to the conclusion that Bob can always learn Alice's committed b with the maximal probability allowed by the trace distance between ρ_0^B and ρ_1^B , while his cheating stands at least 50% chance to escape Alice's detection.

It may look weird that FIG. 1 seems to indicate that the more amount of information that Bob obtains, the easier he can pass Alice's detection. But we must note that the amount of Bob's information is not chosen by himself. Instead, it is determined by the value of α that Alice chooses. That is, once Alice determines which state is used for encoding her committed bit, the maximum amount of information that Bob can obtain is also fixed.

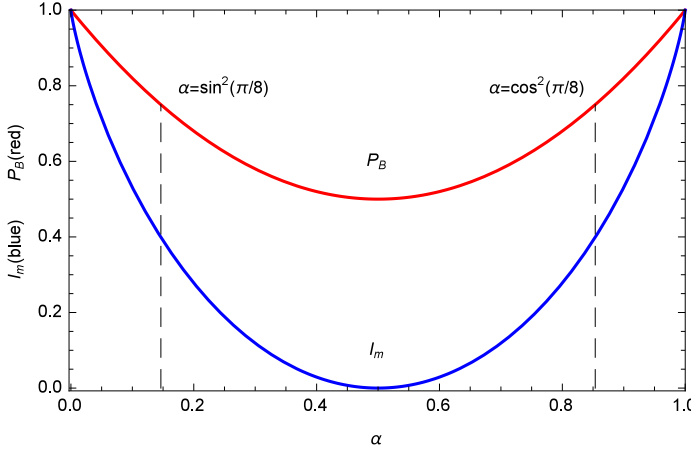


FIG. 1: Bob's successful cheating probability P_B (red line) and mutual information I_m (blue line) on Alice's committed bit b as a function of α that Alice chooses for the initial state Eq. (3). The dash lines mark the values for the protocol in Ref. [5].

On the other hand, the above result indicates that Alice should make α as close to 0.5 as possible, so that Bob's information and successful cheating probability can be minimized. However, note that she has to choose the initial state Eq. (3) within the range restricted by the protocol. Due to the feature (4) of CSQBC, the trace distance $D(\rho_0^B, \rho_1^B)$ has to be nonzero. Therefore, generally α cannot be made very close to 0.5, as we will see in the examples below.

Examples

In the CSQBC protocol in [5], Bob's system Ψ is a single qubit, whose state is either $|0\rangle$ or $|-\rangle$ ($|1\rangle$ or $|+\rangle$) when Alice commits $b = 0$ ($b = 1$). Here $|0\rangle$ and $|1\rangle$ are orthogonal to each other, $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. So we have $\rho_0^B = (|0\rangle\langle 0| + |-\rangle\langle -|)/2$ and $\rho_1^B = (|1\rangle\langle 1| + |+\rangle\langle +|)/2$. Define

$$\begin{aligned} |e^{(0)}\rangle &\equiv \cos(-\pi/8)|0\rangle + \sin(-\pi/8)|1\rangle, \\ |e^{(1)}\rangle &\equiv \cos(3\pi/8)|0\rangle + \sin(3\pi/8)|1\rangle. \end{aligned} \quad (7)$$

Then Bob's operation for maximally discriminating ρ_0^B and ρ_1^B is to measure Ψ in the basis $\{|e^{(0)}\rangle, |e^{(1)}\rangle\}$, i.e., he applies the projector $P_0 = |e^{(0)}\rangle\langle e^{(0)}|$. When the projection is successful (unsuccessful), he takes $b' = 0$ ($b' = 1$) as the decoded result. With this method, b' will match Alice's actual committed bit b with the probability $\cos^2(\pi/8) \simeq 85.36\%$. Meanwhile, Alice's four input

states can be expanded in the $\{|e^{(0)}\rangle, |e^{(1)}\rangle\}$ basis as

$$\begin{aligned} |0\rangle &= \cos(\pi/8)|e^{(0)}\rangle + \sin(\pi/8)|e^{(1)}\rangle, \\ |-\rangle &= \cos(\pi/8)|e^{(0)}\rangle - \sin(\pi/8)|e^{(1)}\rangle, \\ |1\rangle &= -\sin(\pi/8)|e^{(0)}\rangle + \cos(\pi/8)|e^{(1)}\rangle, \\ |+\rangle &= \sin(\pi/8)|e^{(0)}\rangle + \cos(\pi/8)|e^{(1)}\rangle. \end{aligned} \quad (8)$$

Comparing with Eq. (3), we can see that there is either $\alpha = \cos^2(\pi/8)$ or $\alpha = \sin^2(\pi/8)$. Substitute them into Eq. (4) will both yield $P_B = \sin^4(\pi/8) + \cos^4(\pi/8) = 75\%$. That is, in the CSQBC protocol in [5], Bob can learn Alice's committed bit with reliability 85.36% (i.e., his mutual information is $1 - h(0.8536) \simeq 0.4$ bit) before the unveil phase, while he can pass Alice's security check with probability 75%. This protocol is corresponding to the dash lines in our FIG. 1.

Another example can be found in [13], where we illustrated how our above cheating strategy applies on the CSQBC protocol in [9]. This protocol looks more complicated than the one in [5], as the committed bit b is encoded with many qubits, instead of a single one. The authors of [9] merely analyzed the individual attack of the receiver (note that they used the names Alice and Bob reversely) where the qubits are measured one by one. Then it is concluded that the cheating can be detected with a probability arbitrarily close to 1. But as we shown above, instead of individual measurements, the dishonest receiver can apply a two-element POVM $\{P_0^\dagger P_0, P_1^\dagger P_1\}$ on the entire state encoding the committed bit. When this state consists of many qubits, each basis vector $|e_i\rangle$ of the Hilbert space H is a multi-level state describing all qubits. Thus the projectors P_0, P_1 in Eq. (2) are actually collective measurements. The detailed form of P_0, P_1 is given in Eq. (2) of [13]. As a result, it was further elaborated there that this collective measurement is as effective as individual measurements on learning the committed bit, while it causes much less disturbance on the multi-qubit state. Once again, the probability for the cheater to escape the detection was shown [13] to be not less than 50%. With the increase of the qubit number n , this probability can even be arbitrarily close to 100%.

Alice's cheating strategy

Alice's cheating strategy used in the MLC no-go theorem requires the condition $\rho_0^B \simeq \rho_1^B$, which no longer holds in CSQBC. Nevertheless, she can still apply the same strategy in CSQBC and try her luck. To give a detailed description of the strategy, first let us model the coding method in CSQBC more precisely. For generality, consider that in the protocol, besides Bob's system Ψ , there is another system E . Alice's different committed values of b is encoded with different states of the combined system $E \otimes \Psi$. System E is kept at Alice's side

during the commit and holding phases, and is required to be sent to Bob at the unveil phase to justify Alice's commitment. Let ρ_0^{EB} and ρ_1^{EB} denote the density matrices of $E \otimes \Psi$ corresponding to $b = 0$ and $b = 1$, respectively. Note that in all existing CSQBC protocols [5–10], there is no such a system E . But we include it here, so that the model can cover more protocols that may be proposed in the future.

In this scenario, Alice's cheating strategy is as follows. At the beginning of the protocol she introduces an ancillary system Φ which is a copy of $E \otimes \Psi$. Since the fidelity $F(\rho_0^{EB}, \rho_1^{EB}) \equiv \text{tr} \sqrt{(\rho_0^{EB})^{1/2} \rho_1^{EB} (\rho_0^{EB})^{1/2}}$ between ρ_0^{EB} and ρ_1^{EB} satisfies [12]

$$F(\rho_0^{EB}, \rho_1^{EB}) = \max_{|\psi_0\rangle, |\psi_1\rangle} |\langle \psi_0 | \psi_1 \rangle|, \quad (9)$$

where the maximization is over all purifications $|\varphi_0\rangle$ of ρ_0^{EB} and $|\varphi_1\rangle$ of ρ_1^{EB} into $\Phi \otimes E \otimes \Psi$, Alice finds the real and positive $|\psi_0\rangle, |\psi_1\rangle$ that reach the maximum, i.e.,

$$F(\rho_0^{EB}, \rho_1^{EB}) = \langle \psi_0 | \psi_1 \rangle = \langle \psi_1 | \psi_0 \rangle. \quad (10)$$

Then she prepares the initial state of $\Phi \otimes E \otimes \Psi$ as

$$|\psi_c\rangle = \frac{|\psi_0\rangle + |\psi_1\rangle}{N}, \quad (11)$$

where the normalization constant

$$N = \sqrt{2 + \langle \psi_0 | \psi_1 \rangle + \langle \psi_1 | \psi_0 \rangle}. \quad (12)$$

She uses this state to complete the rest of the commit protocol. With this method, the value of b is not determined during the commit phase.

In the unveil phase, Alice decides whether she wants to unveil $b = 0$ or $b = 1$. Then she simply uses $|\psi_c\rangle$ as $|\psi_b\rangle$ to complete the protocol. From the symmetry of $|\varphi_0\rangle$ and $|\varphi_1\rangle$ in Eq.(11), we can see that her successful cheating probabilities for $b = 0$ and $b = 1$ are both

$$\begin{aligned} P_A &= |\langle \psi_0 | \psi_c \rangle|^2 = \frac{(1 + \langle \psi_0 | \psi_1 \rangle)(1 + \langle \psi_1 | \psi_0 \rangle)}{2 + \langle \psi_0 | \psi_1 \rangle + \langle \psi_1 | \psi_0 \rangle} \\ &= \frac{1 + F(\rho_0^{EB}, \rho_1^{EB})}{2}. \end{aligned} \quad (13)$$

Therefore, in any specific CSQBC protocol, the Alice's exact cheating probability can be calculated once the definition of ρ_0^{EB}, ρ_1^{EB} is known.

The optimal protocols are trivial

Now we will try to find the CSQBC protocols which can optimally detect the cheating of both parties, i.e., minimizing the sum of Alice's and Bob's cheating probabilities.

Note that Eq. (4) depends on the specific value of α in the state Eq. (3) that Alice chooses in a single run of the protocol, while $F(\rho_0^{EB}, \rho_1^{EB})$ in Eq. (13) is the statistical

result of all the legitimate states allowed by the protocol. Thus it is hard to compare Eq. (13) and Eq. (4) directly and give a general result without knowing the details on the composition of ρ_b^{EB} in a specific protocol.

Fortunately, in all existing CSQBC protocols [5–10], there is no system E . The form of the states of Bob's system Ψ alone carries all the information of b . Thus the trace distance $D(\rho_0^{EB}, \rho_1^{EB}) = D(\rho_0^B, \rho_1^B)$. For any protocol of this kind (as well as protocols having system E but still satisfying $D(\rho_0^{EB}, \rho_1^{EB}) = D(\rho_0^B, \rho_1^B)$), we can replace both α and $F(\rho_0^{EB}, \rho_1^{EB})$ with $D(\rho_0^B, \rho_1^B)$, as elaborated in the 2nd subsection of Method, where we obtain

$$P_A \geq 1 - \frac{D(\rho_0^B, \rho_1^B)}{2}, \quad (14)$$

and

$$P_B \geq \frac{1 + D(\rho_0^B, \rho_1^B)^2}{2}. \quad (15)$$

These two equations suggest that P_A and P_B cannot be minimized simultaneously in the same protocol, because reducing P_A requires a higher $D(\rho_0^B, \rho_1^B)$, while it will result in a higher P_B at the same time.

Moreover, we must note that the above P_A and P_B are obtained assuming that the actions of both parties in the protocol will always be checked. But this is impossible, because they share the same system $\Phi \otimes E \otimes \Psi$. In the unveil phase, either Bob will measure $E \otimes \Psi$ to check Alice's action, or he is required to return Ψ to Alice who checks his action. These cannot be done simultaneously. Suppose that in a CSQBC protocol, Bob's action is checked with probability ζ ($0 \leq \zeta \leq 1$), and Alice's action is checked with probability $1 - \zeta$. When one's action is not checked, he/she can cheat successfully with probability 1. Thus the cheating probabilities P_A and P_B should be replaced by

$$P_A^* = \zeta + (1 - \zeta)P_A \quad (16)$$

and

$$P_B^* = (1 - \zeta) + \zeta P_B, \quad (17)$$

respectively. Combining them with Eqs. (14) and (15), we find

$$\begin{aligned} P_A^* + P_B^* &\geq 2 - \frac{\zeta + D(\rho_0^B, \rho_1^B)}{2} \\ &\quad + \zeta D(\rho_0^B, \rho_1^B) \frac{1 + D(\rho_0^B, \rho_1^B)}{2}. \end{aligned} \quad (18)$$

Since $0 \leq \zeta \leq 1$ and $0 \leq D(\rho_0^B, \rho_1^B) \leq 1$, we find another security lower bound of CSQBC

$$P_A^* + P_B^* \geq \frac{3}{2}. \quad (19)$$

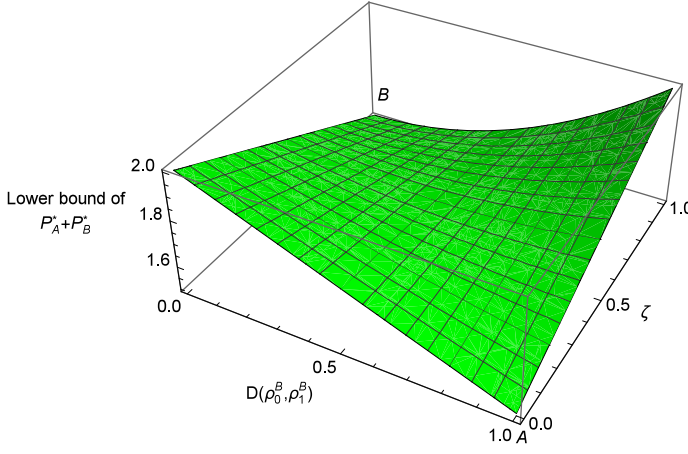


FIG. 2: The lower bound of the sum of the cheating probabilities $P_A^* + P_B^*$ as a function of the trace distance $D(\rho_0^B, \rho_1^B)$ and the probability ζ with which Bob's action is checked. A and B denote the points that reach the minimum $P_A^* + P_B^* = 3/2$.

To find the optimal protocol that can reach this bound, we plot the lower bound of $P_A^* + P_B^*$ as a function of $D(\rho_0^B, \rho_1^B)$ and ζ in FIG. 2 according to Eq. (18). It shows that there are two types of protocols that can both reach the minimum $P_A^* + P_B^* = 3/2$, denoted as points A and B in FIG. 2, respectively, with the parameters (A) $D(\rho_0^B, \rho_1^B) = 1$, $\zeta = 0$, and (B) $D(\rho_0^B, \rho_1^B) = 0$, $\zeta = 1$. Type (A) protocols mean that ρ_0^B and ρ_1^B are orthogonal so that P_A^* reaches its minimum $1/2$. However, ρ_0^B and ρ_1^B can be distinguished perfectly and Bob's action is never checked. Thus $P_B^* = 1$, i.e., he can always learn Alice's committed b with reliability 1 and never get caught. In type (B) protocols, $\rho_0^B = \rho_1^B$ so that Bob learns nothing about b . But Alice's action is never checked so that she can unveil b as whatever she wants, with a successful cheating probability $P_A^* = 1$. Therefore, we can see that these optimal protocols are all trivial as they are completely insecure against one of the parties. Thus they do not seem to have any practical usage.

The fair protocol

Since the protocols that can minimize $P_A^* + P_B^*$ all look useless, let us consider the protocol satisfying $P_A^* = P_B^*$ so that it is fair for both parties, and try to minimize P_A^*, P_B^* in this case. From Eq. (37) we can see that the inequality Eq. (15) can become equality when $\bar{\alpha}^2 = \alpha^2$, i.e., all the states allowed to be chosen in the protocol for committing the same b value should have the same α value. Also, note that the lowest bounds in Eqs. (14) and (18) cannot be reached by most $D(\rho_0^B, \rho_1^B)$, because these inequalities can become equalities if and only if $F(\rho_0^B, \rho_1^B) = 1 - D(\rho_0^B, \rho_1^B)$, which requires $\rho_0^B = \rho_1^B$. Therefore, only the above optimal protocols can reach these bound. For this reason, to calculate P_A^* precisely in other protocols, we should use Eq. (13) instead of Eq.

(14). To compute $F(\rho_0^{EB}, \rho_1^{EB})$ in Eq. (13), for simplicity we consider only the protocols in which there are

$$\begin{aligned}\rho_0^{EB} &= \rho_0^B = \begin{bmatrix} \alpha & 0 \\ 0 & 1 - \alpha \end{bmatrix}, \\ \rho_1^{EB} &= \rho_1^B = \begin{bmatrix} 1 - \alpha & 0 \\ 0 & \alpha \end{bmatrix},\end{aligned}\quad (20)$$

then

$$\begin{aligned}F(\rho_0^B, \rho_1^B) &= 2\sqrt{\alpha(1 - \alpha)}, \\ D(\rho_0^B, \rho_1^B) &= 2\alpha - 1.\end{aligned}\quad (21)$$

Combining them with Eqs. (13), (16), (17) and (15) (the latter becomes equality once we choose $\bar{\alpha}^2 = \alpha^2$), then by solving $P_A^* = P_B^*$ we yield

$$\zeta = \frac{2\sqrt{\alpha(1 - \alpha)} - 1}{(2\alpha - 1)^2 + 2\sqrt{\alpha(1 - \alpha)} - 2}.\quad (22)$$

Any protocol satisfying this equation is fair for both parties. Now let us find the minimal value of $P_A^* = P_B^*$. Substituting this ζ into Eq. (17), we obtain

$$P_A^* = P_B^* = \frac{(2\sqrt{\alpha(1 - \alpha)} + 1)(2\alpha^2 - 2\alpha + 1) - 2}{4\alpha^2 - 4\alpha + 2\sqrt{\alpha(1 - \alpha)} - 1}.\quad (23)$$

By solving $dP_A^*/d\alpha = 0$, we find that the minimal cheating probabilities in such protocols are $P_A^* = P_B^* = 0.904$, which can be obtained when $\alpha \simeq 0.885$, i.e., $\sqrt{\alpha} \simeq 0.941 \simeq \cos(19.85^\circ)$. In this case $\zeta \simeq 0.469$.

A simple protocol having these parameters is: Alice sends Bob the state $\cos(19.85^\circ)|0\rangle \pm \sin(19.85^\circ)|1\rangle$ ($\sin(19.85^\circ)|0\rangle \pm \cos(19.85^\circ)|1\rangle$) if she wants to commit $b = 0$ ($b = 1$). In the unveil phase, with probability $\zeta \simeq 0.469$ Bob returns the state and Alice checks whether it remains undisturbed, with probability $1 - \zeta \simeq 0.531$ Bob measures the state and checks whether it agrees with the value of Alice unveiled b .

Nevertheless, there is the difficulty in finding a method for deciding which party will be checked in a single run of the protocol. Dishonest Alice (Bob) would like to decrease $1 - \zeta$ (ζ) so that P_A^* (P_B^*) can be raised. Thus they do not trust each other and may not collaborate. The CSQBC protocol in [5] adopts a process called "the game" to handle this problem, which is very similar to quantum coin flipping (QCF) protocols [14]. However, Ishizaka [15] showed that this process provides extra security loophole to Bob, so that there is a cheating strategy for him to learn b with reliability 61.79% (which is lower than what can be obtained with our cheating strategy, as calculated in the Examples section) while passing Alice's check with probability 100% (which is higher than that of our strategy). It was further shown in [16] that due to the inexistence of ideal black-boxed QCF, any CSQBC protocol based on biased QCF cannot be secure. Therefore, it remains unclear how to build a fair CSQBC protocol with $P_A^* = P_B^*$ while minimizing P_A^* and P_B^* .

Discussion

In summary, we showed that any CSQBC protocol having the above four features is subjected to the security bound Eq. (6). Protocols satisfying $D(\rho_0^{EB}, \rho_1^{EB}) = D(\rho_0^B, \rho_1^B)$ is further bounded by Eq. (19). Note that the insecurity of QCF-based CSQBC protocols (e.g., [5, 6]) was already pinpointed out in [15, 16]. But our proof also applies to the non-QCF-based ones.

Our result should not be simply considered as a generalization of the MLC no-go proof. Instead, it is a complement. This is because the MLC no-go proof applies to QBC protocol with $\rho_0^B \simeq \rho_1^B$. But as pointed out in [9], CSQBC does not need to satisfy this requirement so that it may evade the MLC theorem. On the contrary, our proof works for the case $\rho_0^B \neq \rho_1^B$, thus it fills the gap where the MLC proof left. Meanwhile, the MLC theorem concentrates on the cheating of Alice. It does not exclude the existence of protocols which is unconditionally secure against dishonest Bob only. On the other hand, our result shows that Bob can always cheat in CSQBC regardless Alice is honest or not.

It will be interesting to study whether there can be CSQBC protocols without the above four features. It seems that Kent's relativistic QBC [17–19] and our recent proposals [20, 21] do not satisfy feature (1), while the protocol in [22] does not have feature (2), as elaborated in [23]. However, these works are aimed to achieve the original QBC, instead of CSQBC. Also, [20–23] have not gained wide recognition yet. Thus it is still an open question whether it is possible to build non-relativistic CSQBC protocols which are not limited by the above security bounds, without relying on computational and experimental constraints.

Methods

Calculating Bob's cheating probability

Consider the POVM $\{P_0^\dagger P_0, P_1^\dagger P_1\}$ defined in Eq. (2). After Bob applies it on Ψ , there can be two outcomes.

(I) The projection outcome is P_0 . Then Bob takes $b' = 0$ as his decoded result of Alice's committed bit b . With Eqs. (2) and (3) we yield

$$P_0 |\Phi \otimes \Psi\rangle_{ini} = \sqrt{\alpha} \sum_i \lambda_i^{(0)} |f_i^{(0)}\rangle \otimes |e_i^{(0)}\rangle. \quad (24)$$

Thus this case will occurs with the probability

$$p_I = \alpha, \quad (25)$$

while the resultant state of $\Phi \otimes \Psi$ is

$$|\Phi \otimes \Psi\rangle_I = \frac{1}{\sqrt{p_I}} P_0 |\Phi \otimes \Psi\rangle_{ini}. \quad (26)$$

As described in feature (3) of CSQBC, at the unveil phase Alice may require Bob to return Ψ and check

whether it remains intact in its initial state. The maximal probability for Alice to find out that Bob has already projected $|\Phi \otimes \Psi\rangle_{ini}$ into $|\Phi \otimes \Psi\rangle_I$ is bounded by

$$\begin{aligned} \tilde{p}_I &= 1 - |{}_I \langle \Phi \otimes \Psi | \Phi \otimes \Psi \rangle_{ini}|^2 \\ &= 1 - \frac{1}{p_I} \alpha^2. \end{aligned} \quad (27)$$

Thus the total probability for (case (I) occurred) AND (Alice failed to detect Bob's cheating) is

$$p_I(1 - \tilde{p}_I) = \alpha^2. \quad (28)$$

(II) The projection outcome is P_1 . Then Bob takes $b' = 1$ as his decoded result of Alice's b . Now

$$P_1 |\Phi \otimes \Psi\rangle_{ini} = \sqrt{\beta} \sum_i \lambda_i^{(1)} |f_i^{(1)}\rangle \otimes |e_i^{(1)}\rangle. \quad (29)$$

Obviously, this case will occurs with the probability

$$p_{II} = 1 - p_I. \quad (30)$$

Meanwhile, the resultant state of $\Phi \otimes \Psi$ in this case is

$$|\Phi \otimes \Psi\rangle_{II} = \frac{1}{\sqrt{p_{II}}} P_1 |\Phi \otimes \Psi\rangle_{ini}. \quad (31)$$

The maximal probability for Alice to find out that Bob has already projected $|\Phi \otimes \Psi\rangle_{ini}$ into $|\Phi \otimes \Psi\rangle_{II}$ is bounded by

$$\begin{aligned} \tilde{p}_{II} &= 1 - |{}_{II} \langle \Phi \otimes \Psi | \Phi \otimes \Psi \rangle_{ini}|^2 \\ &= 1 - \frac{1}{p_{II}} \beta^2. \end{aligned} \quad (32)$$

Thus the total probability for (case (II) occurred) AND (Alice failed to detect Bob's cheating) is

$$p_{II}(1 - \tilde{p}_{II}) = \beta^2. \quad (33)$$

Taking both cases (I) and (II) into consideration, the overall probability for Bob's cheating to pass Alice's detection successfully is

$$\begin{aligned} P_B &= p_I(1 - \tilde{p}_I) + p_{II}(1 - \tilde{p}_{II}) = \alpha^2 + \beta^2 \\ &= \frac{1}{2} + \frac{1}{2}(2\alpha - 1)^2. \end{aligned} \quad (34)$$

Meanwhile, since the projection outcome will either be P_0 or P_1 with the probabilities p_I and $p_{II} = 1 - p_I$, respectively, Bob's b' will match Alice's b with the probability p_I or $1 - p_I$ too. Note that $h(1 - p_I) = h(p_I)$. Thus the amount of mutual information that Bob obtains with this POVM is

$$I_m = 1 - h(p_I) = 1 - h(\alpha). \quad (35)$$

Bounding the cheating probabilities with trace distance

Suppose that there are many states allowed to be chosen randomly for committing $b = 0$ in the protocol, each of which takes the form of Eq. (3), but with different values of the coefficients α , β , $\lambda_i^{(0)}$'s and $\lambda_i^{(1)}$'s. Bob applies the optimal POVM to decode b . Then Eq. (3) indicates that he can learn b correctly with probability $\bar{\alpha}$, i.e., the average of α . Meanwhile, it is well-known that the maximal probability for discriminating two density matrices ρ_0^B , ρ_1^B is $(1 + D(\rho_0^B, \rho_1^B))/2$. Therefore

$$D(\rho_0^B, \rho_1^B) = 2\bar{\alpha} - 1. \quad (36)$$

Since Eq. (4) shows that Bob's average cheating probability for these states is

$$P_B = \frac{1 + \overline{(2\alpha - 1)^2}}{2} \geq \frac{1 + (2\bar{\alpha} - 1)^2}{2}, \quad (37)$$

we have

$$P_B \geq \frac{1 + D(\rho_0^B, \rho_1^B)^2}{2}. \quad (38)$$

Similar discussion is also valid for the states for committing $b = 1$, except that α should be replaced by $\beta = 1 - \alpha$. But Eq. (38) remains the same because Eq. (4) satisfies $P_B(1 - \alpha) = P_B(\alpha)$.

On the other hand, since [12]

$$F(\rho_0^B, \rho_1^B) \geq 1 - D(\rho_0^B, \rho_1^B), \quad (39)$$

from Eq. (13) we yield

$$P_A \geq 1 - \frac{D(\rho_0^B, \rho_1^B)}{2}. \quad (40)$$

-
- [1] Yao, A. C. C. Security of quantum protocols against coherent measurements. In *Proc. 26th Symposium on the Theory of Computing*. New York: ACM, pp. 67. (1995).
- [2] Kilian, J. Founding cryptography on oblivious transfer. In *Proc. 1988 ACM Annual Symposium on Theory of Computing*. New York: ACM, pp. 20. (1988).
- [3] Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **78**, 3414 (1997).
- [4] Lo, H. -K. & Chau, H. F. Is quantum bit commitment really possible? *Phys. Rev. Lett.* **78**, 3410 (1997).
- [5] Hardy, L. & Kent, A. Cheat sensitive quantum bit commitment. *Phys. Rev. Lett.* **92**, 157901 (2004).
- [6] Aharonov, D., Ta-Shma, A., Vazirani, U. V. & Yao, A. C. Quantum bit escrow. *arXiv:quant-ph/0004017v1*. In *Proc. 32nd Annual Symposium on Theory of Computing*. New York: ACM, pp. 705. (2000).
- [7] Jakoby, A., Liskiewicz, M. & Madry, A. Using quantum oblivious transfer to cheat sensitive quantum bit commitment. *arXiv:quant-ph/0605150v1* (2006).
- [8] Buhrman, H., Christandl, M., Hayden, P., Lo, H. -K. & Wehner, S. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Phys. Rev. A* **78**, 022316 (2008).
- [9] Shimizu, K., Fukasaka, H., Tamaki, K. & Imoto, N. Cheat-sensitive commitment of a classical bit coded in a block of $m \times n$ round-trip qubits. *Phys. Rev. A* **84**, 022308 (2011).
- [10] Li, Y. -B., Wen, Q. -Y., Li, Z. -C., Qin, S. -J. & Yang, Y. -T. Cheat sensitive quantum bit commitment via pre- and post-selected quantum states. *Quant. Inf. Process.* **13**, 141 (2014).
- [11] Hughston, L. P., Jozsa, R. & Wootters, W. K. A complete classification of quantum ensembles having a given density matrix. *Phys. Lett. A* **183**, 14 (1993).
- [12] Nielsen, M. A. & Chuang, I. L. in *Quantum computation and quantum information*, Ch. 9.2, 404-416 (Cambridge, 2000).
- [13] He, G. P. Comment on "Cheat-sensitive commitment of a classical bit coded in a block of $m \times n$ round-trip qubits". *Phys. Rev. A* **89**, 056301 (2014).
- [14] Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, 175 (IEEE Press, New York, 1984).
- [15] Ishizaka, S. Is cheat sensitive quantum bit commitment really possible? *arXiv:quant-ph/0703099v3* (2007).
- [16] Ishizaka, S. Dilemma that cannot be resolved by biased quantum coin flipping. *Phys. Rev. Lett.* **100**, 070501 (2008).
- [17] Kent, A. Unconditionally secure bit commitment. *Phys. Rev. Lett.* **83**, 1447 (1999).
- [18] Kent, A. Unconditionally secure bit commitment with flying qubits. *New J. Phys.* **13**, 113015 (2011).
- [19] Kent, A. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.* **109**, 130501 (2012).
- [20] He, G. P. Quantum key distribution based on orthogonal states allows secure quantum bit commitment. *J. Phys. A: Math. Theor.* **44**, 445305 (2011).
- [21] He, G. P. Simplified quantum bit commitment using single photon nonlocality. *Quantum Inf. Process.* **13**, 2195 (2014).
- [22] He, G. P. Secure quantum bit commitment against empty promises. *Phys. Rev. A* **74**, 022332 (2006).
- [23] He, G. P. Secure quantum bit commitment against empty promises. II. The density matrix. *arXiv:1307.7318* (2013).

Acknowledgements

The work was supported in part by the NSF of China, the NSF of Guangdong province, and the Foundation of Zhongshan University Advanced Research Center.

Additional information

Competing financial interests: The author declares no competing financial interests.